

Figure 1

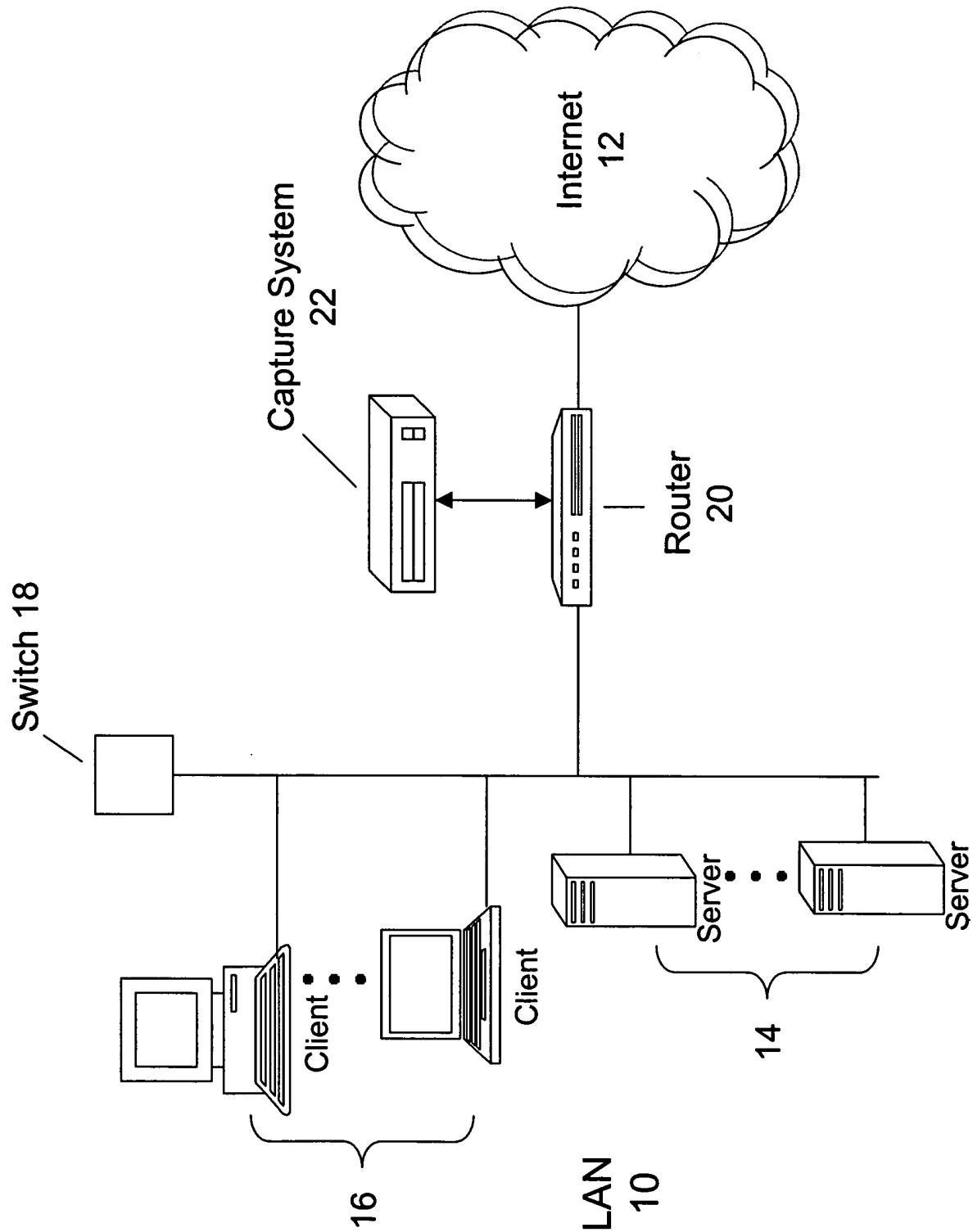


Figure 2

Capture System 22

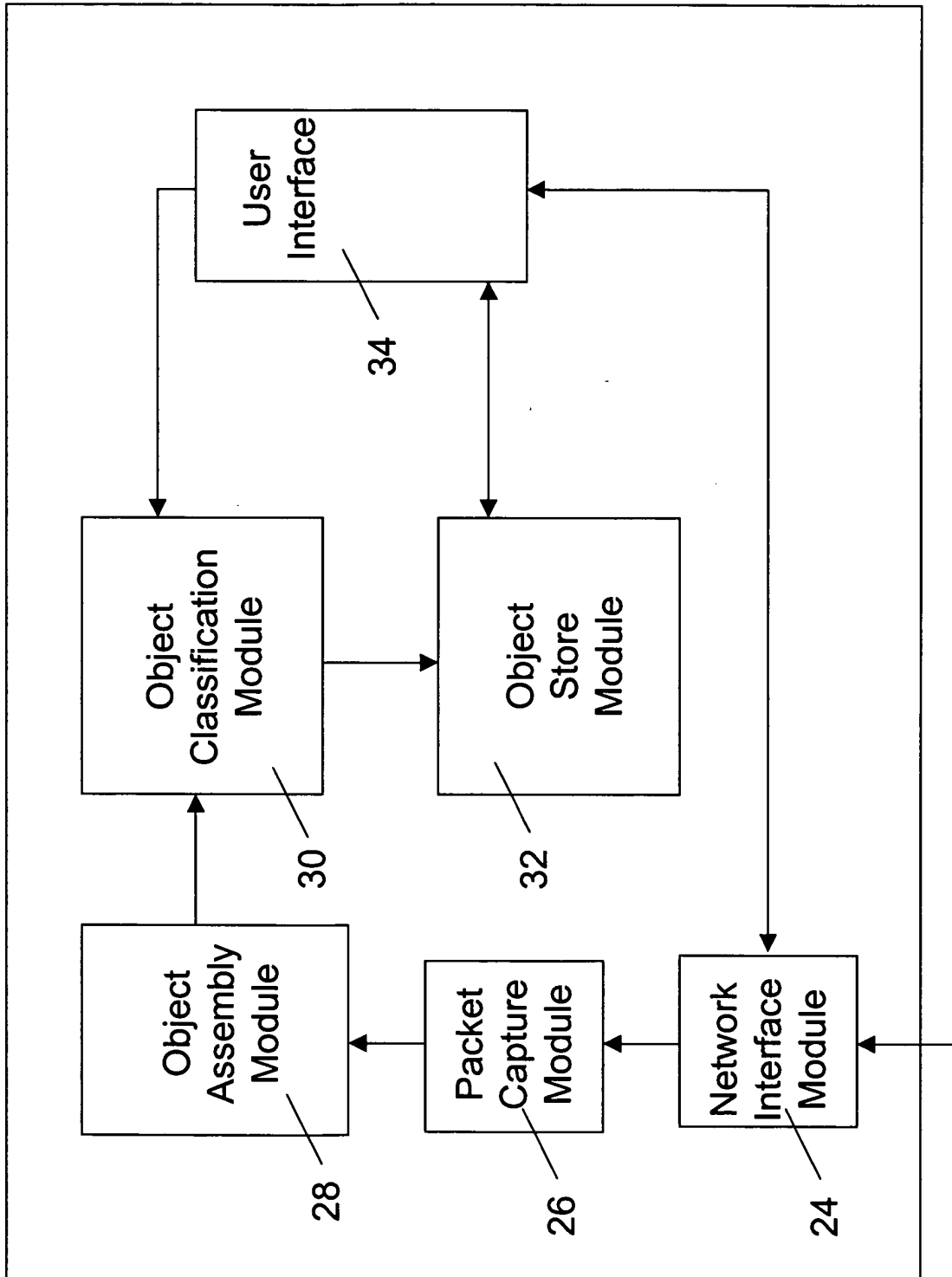


Figure 3

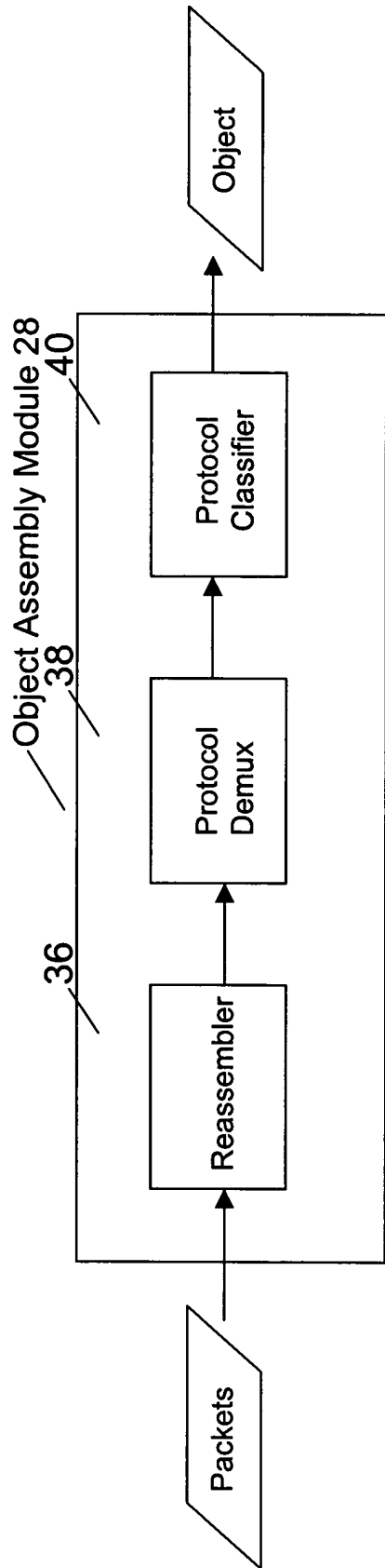


Figure 4

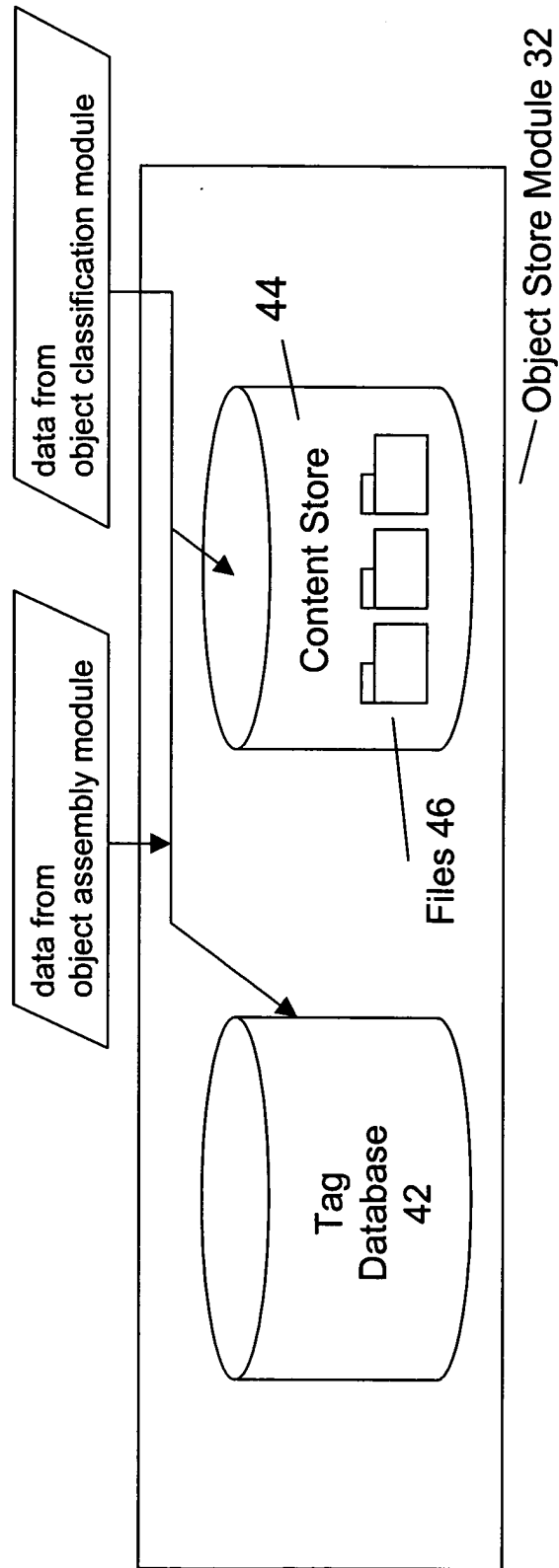


Figure 5

Capture System 22

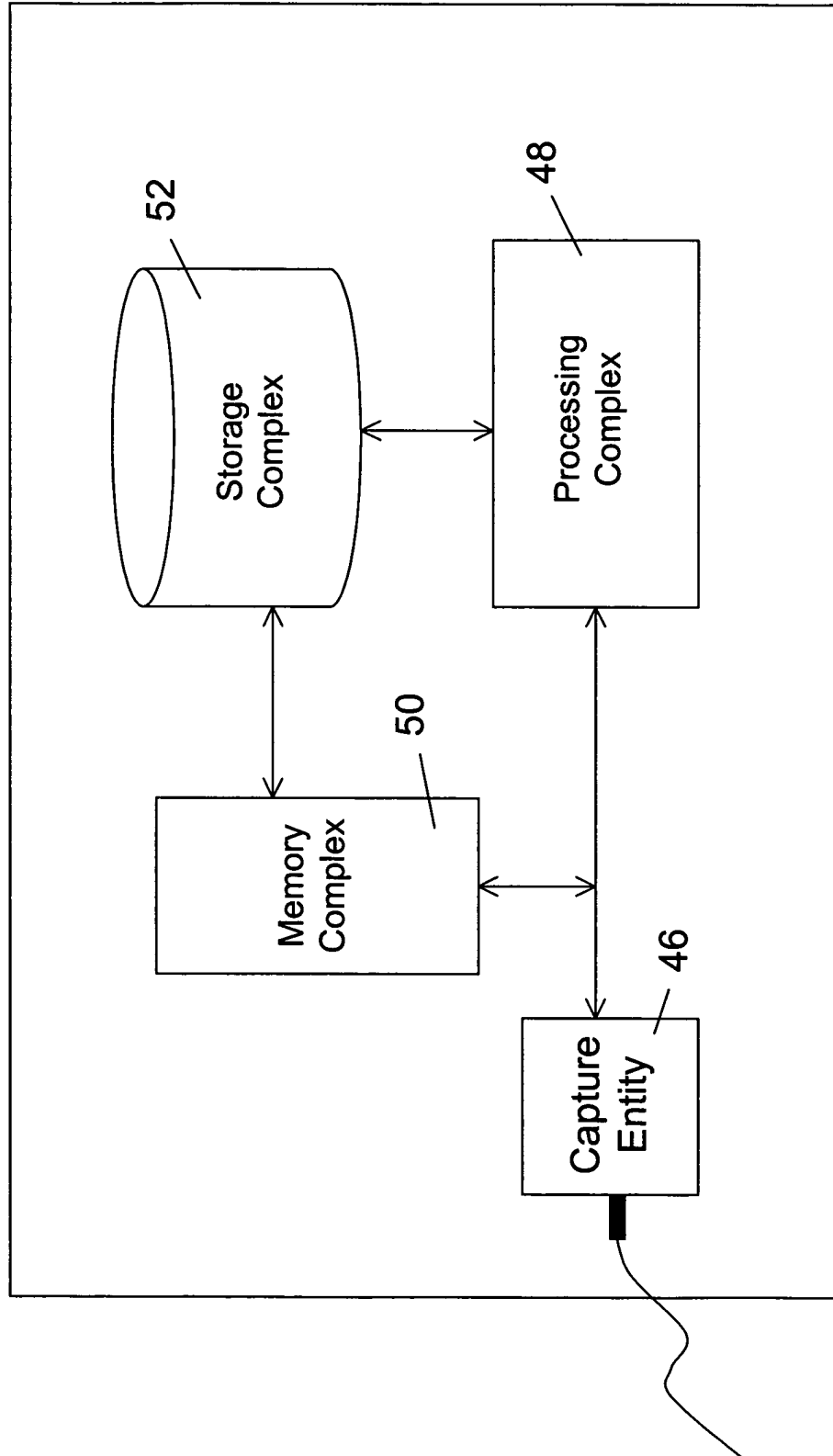


Figure 6

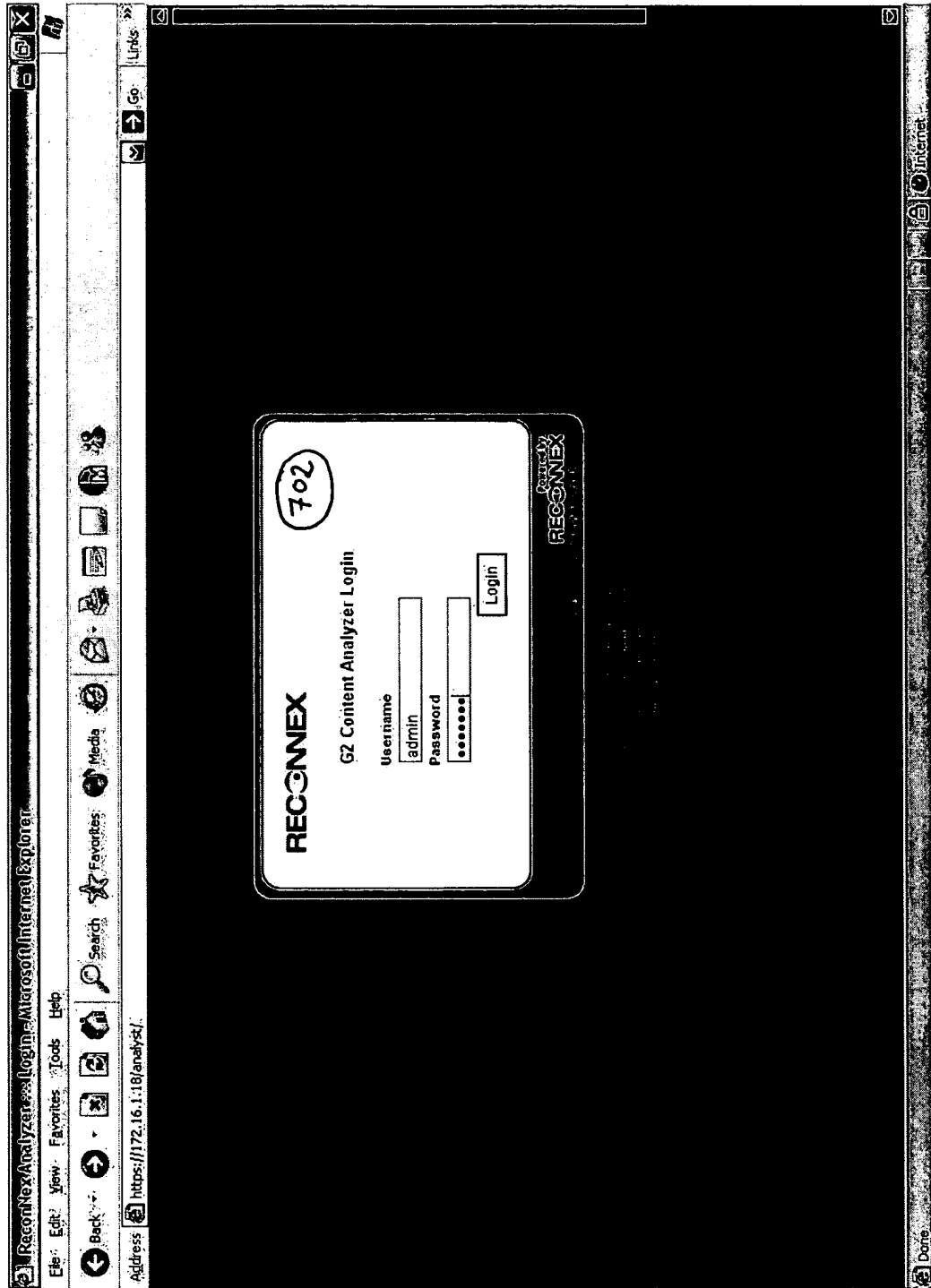


Figure 7

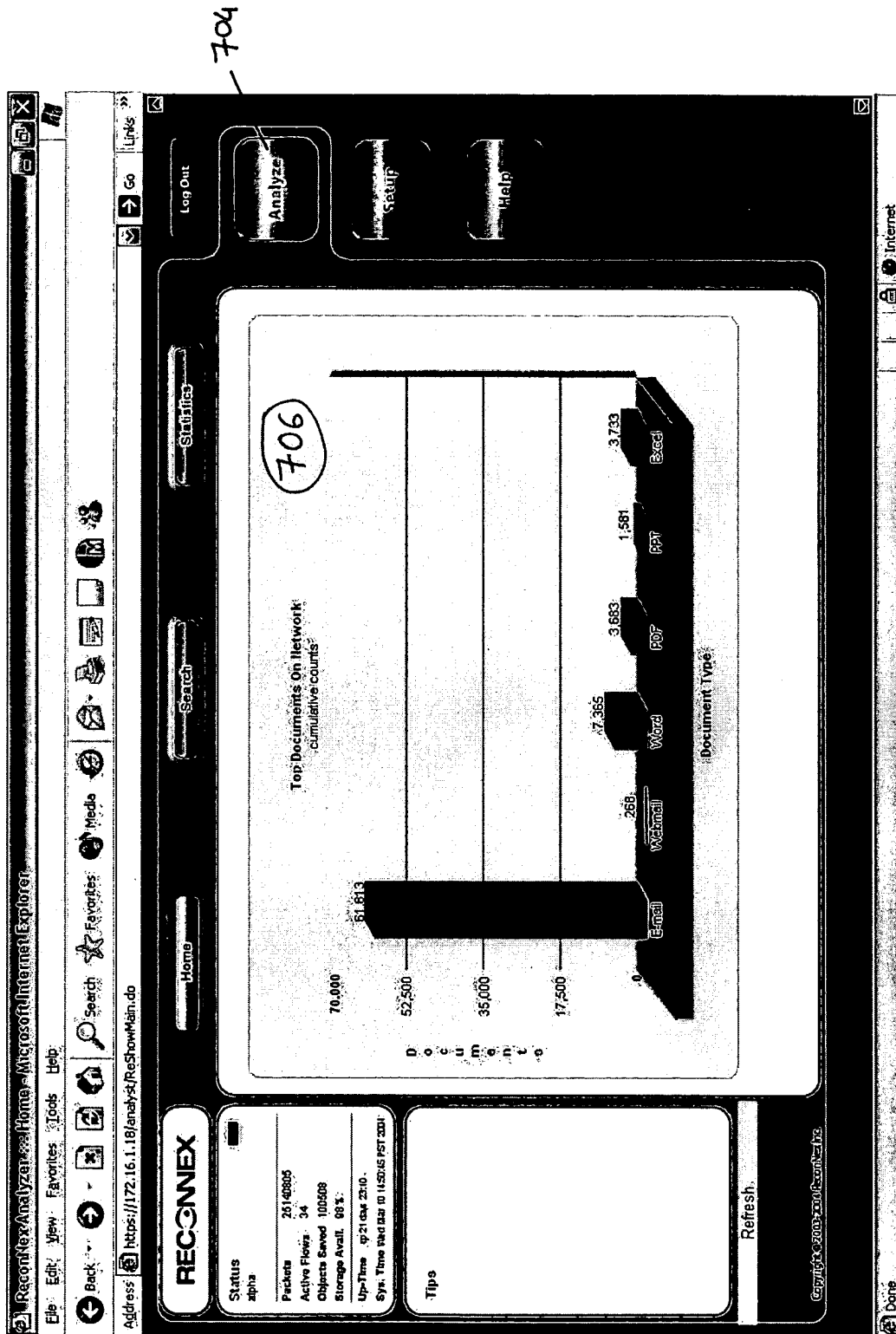


Figure 8

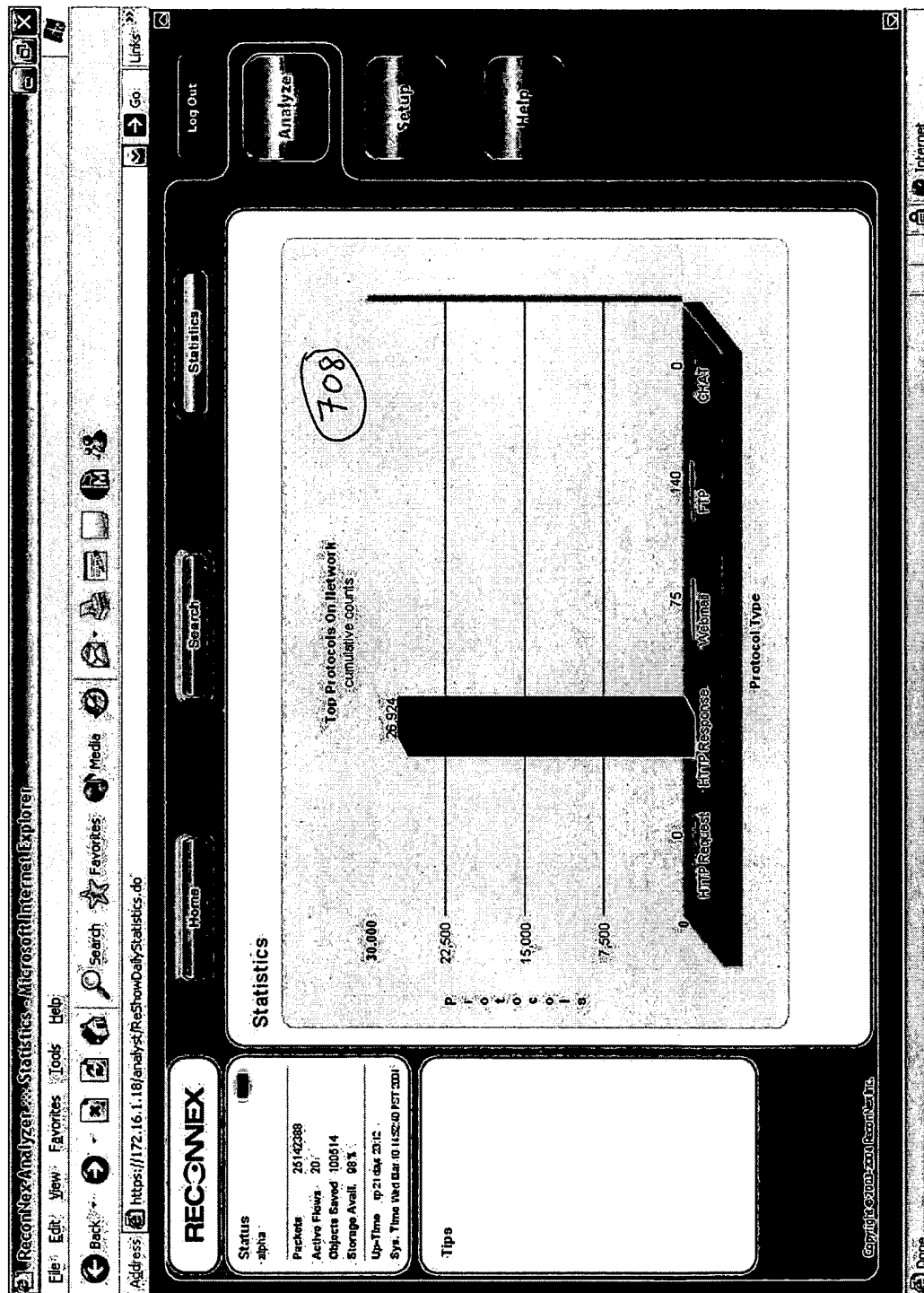


Figure 9

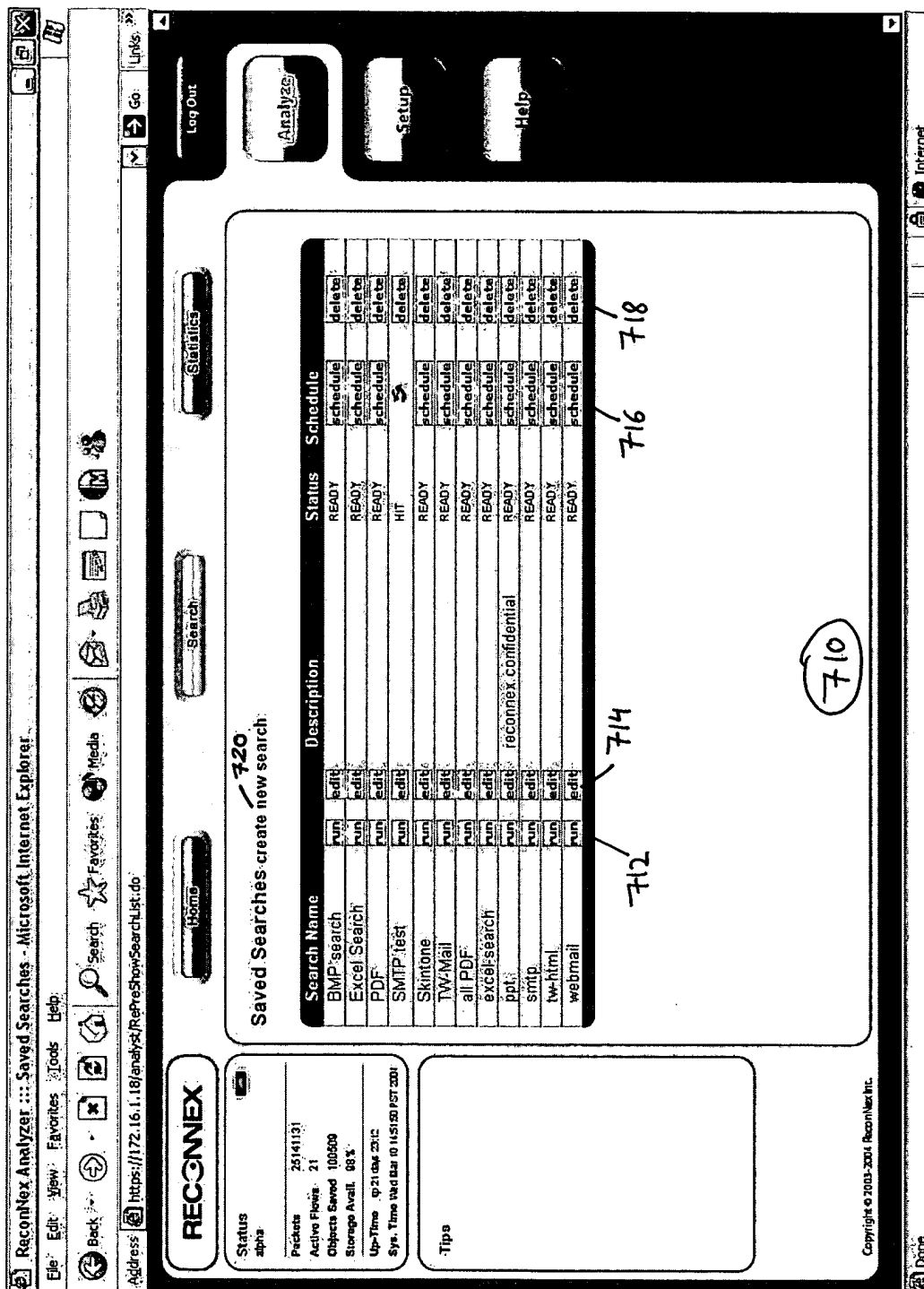


Figure 10

ReconNex Analyzer v1.18 / New Documents Search - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address: https://172.16.1.18/analyzer/ReconNexSearchDocNow.do?method=call=modifySearch&searchName=PDF

Log Out Analyze Setup Help

Home Search Statistics

Create Search back to Saved Searches

Documents

Mail

Images

FTP

Words to search: etheral with all of the words
 with the exact phrase
 with at least one of the words

Source IP Mask Port From to
 Destination IP Mask Port From to

Type: Excel HTML MSWord PDF
 Protocol: HTTP Post HTTP Response HTTP Webmail Attach SMTP Attach

Size: To 1024, 200K, or 1.5M
 Date/Time From [pick] Time [mmddyyyy - hh:mm]
 Date/Time To [pick] Time [pick]

Save Search: Name PDF Description

722

RECONNEX

Status: alpha

Packets: 25144706

Active Flows: 42

Objects Saved: 100314

Storage Avail: 88%

Up Time: 621 days 21:13

Sys. Time Wed Mar 10 11:53:25 PST 2004

Tips

Copyright 2002-2004 ReconNex, Inc.

Figure 11

ReconNexAnalyzer - New Mail Search - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address: https://172.16.1.18/analyze/ReCreateSearchMailNow.do?method=call=modifySearch&searchName=TW-Mail

Log Out Analyze Setup Help

Statistics Search Home

Create Search back to Saved Searches

Documents Mail WebMail SMTP FTP Images

Type

Address From To

Cc Bcc

Subject

Message Keywords

Size To 1024, 2048, or 15m

Date/Time From [pick] Time [pick] Time [pick] Time [pick]

Date/Time To [pick] Time [pick]

Save Search

Name TW-Mail

Description

Define Search

722

RECONNEX

Status alpha

Packets 2514604

Active Flows 34

Objects Saved 100514

Storage Avail. 98%

Up-Time 921 day 23:14

Sys. Time Wed Mar 10 11:51:17 PST 2004

Tips

Copyright 2000-2004 ReconNex, Inc.

Figure 12

ReconNex Analyzer - New Image Search - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address: https://172.16.1.18/anahst/ReCreateSearchImpNow.do?methodocal=modifySearch&searchName=Bmp+search

Log Out Analyze Setup Help

Home Search Status

Create Search back to Saved Searches

Documents Mail Images FTP

Skin Tone Analyzer On Off

Source IP: Mask Port From: to: Mask Port From: to: Mask Port From: to: Mask Port From: to:

Destination IP: Mask Port From: to: Mask Port From: to: Mask Port From: to: Mask Port From: to:

Type Bmp GIF JPEG Protocol HTTP Post HTTP Response HTTP Webmail Attach SMTP Attach

Size To: 1024:200k; or 15m

Date/Time From: [pick] Time: [pick] Time: [pick]

Date/Time To: [pick] Time: [pick] Time: [pick]

Save Search Name Bmp search Description

Define Search

722

RECONNEX

Status alpha

Packets 25148224

Active Flows 18

Objects Saved 10218

Storage Avail. 98 %

Up Time 421 d 21 h 23 m

Sys. Time Wed Oct 10 11:51:57 PST 2001

Tips

Copyright 2000-2001 ReconNex, Inc.

Done

Figure 13

ReconNexAnalyzer...<...beammessagekey-http:search.html?...>Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address <https://172.16.1.18/analyst/ReCreateSearchFTP.do>

Log Out Analyze Setup Help

Search

Create Search back to Saved Searches

Documents Mail Images FTP

Source IP: Mask:
Destination IP: Mask:
User Name:
Transmit Keywords:
Receive Keywords:
Size: To: 1024, 200K, or 1.5M
Date/Time From: (pick) Time: (mm/dd/yyyy) (hh:mm)
Date/Time To: (pick) Time: (mm/dd/yyyy) (hh:mm)

Save Search

Name:
Description:

Define Search

722

RECONNEX

Status: alpha

Packets: 25140074
Active Flows: 20
Objects Saved: 100020
Storage Avail: 0%

Up Time: 02:21:04:23:16
Sys. Time: 10/10/2001 11:55:59 PST 2001

Tip

Copyright © 2000-2001 ReconNex, Inc.

Done

Figure 14

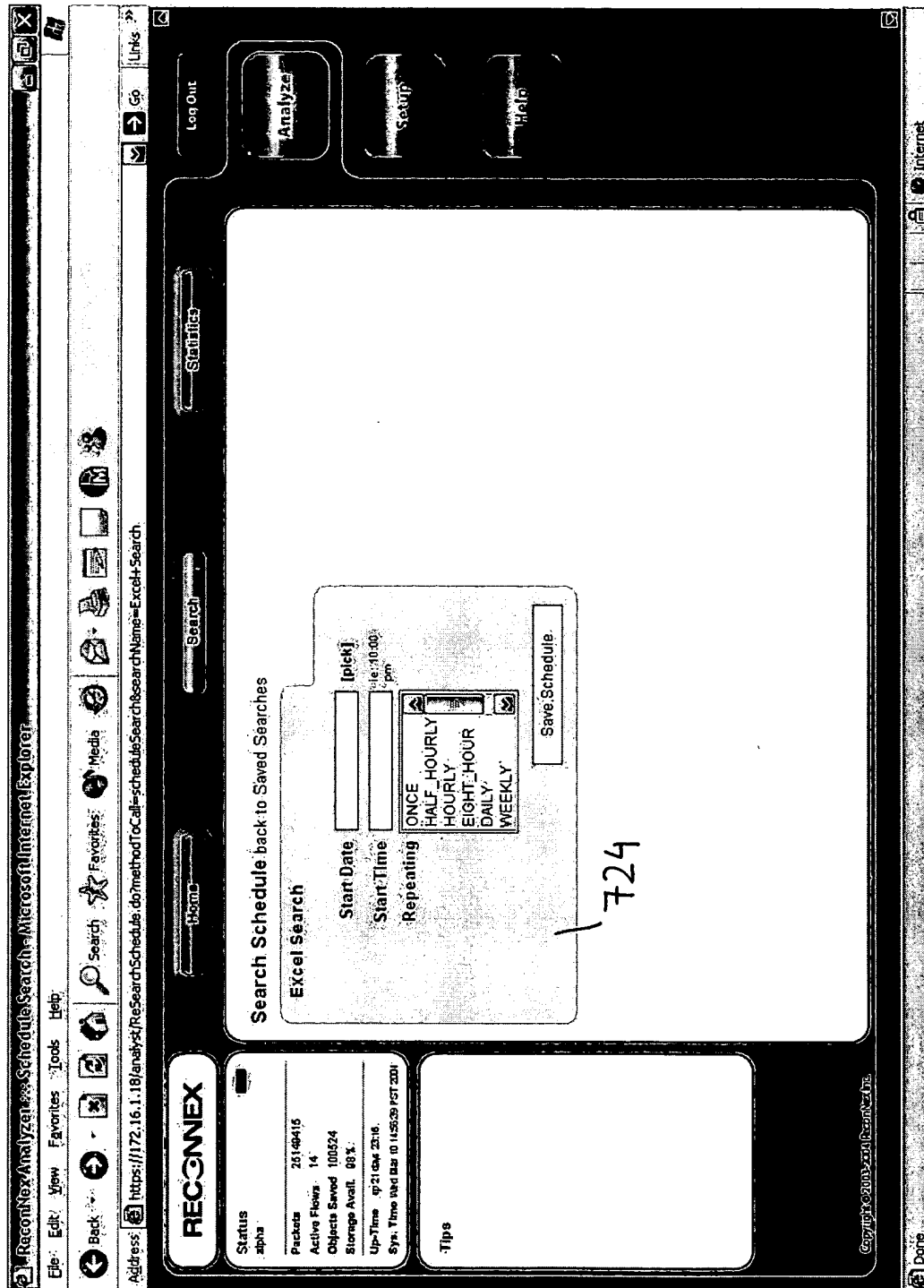


Figure 15

ReconNex Analyzer - Search Results - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address <https://172.16.1.18/analyt/ReCreateSearchNow.do?methodToCall=getSearchResults&searchName=PDF>

Log Out Analyze Setup Help

Search

Search Results back to Saved Searches

Search Name PDF

Type	Content	Source	Destination	Size	Date
PDF	19c3-hijackersguide.pdf	212.227.109.200	172.16.1.41	304704	03/19/2004 19:31:07
PDF	arch_wp.pdf	64.124.140.199	172.16.1.41	301817	03/19/2004 15:46:22
PDF	arch_wp.pdf	64.124.140.199	172.16.1.41	96	03/19/2004 15:46:13
PDF	arch_wp.pdf	64.124.140.199	172.16.1.41	1024	03/19/2004 15:46:13
PDF	arch_wp.pdf	64.124.140.199	172.16.1.41	1024	03/19/2004 15:46:13
PDF	arch_wp.pdf	64.124.140.199	172.16.1.41	1024	03/19/2004 15:46:08
PDF	Ring.pdf	131.114.21.22	172.16.1.95	224562	03/17/2004 17:53:50
PDF	Site-Survey-Form.pdf	129.41.63.39	172.16.1.93	68800	03/17/2004 17:41:55
Unknown	Unknown	20.0.0.110	172.16.1.23	3351541	03/16/2004 10:05:02
Unknown	Unknown	20.0.0.110	172.16.1.23	3351541	03/16/2004 10:02:35
Unknown	Unknown	20.0.0.110	172.16.1.23	3351541	03/16/2004 10:00:08
Unknown	Unknown	20.0.0.110	172.16.1.23	3351541	03/16/2004 09:57:39
Unknown	Unknown	20.0.0.110	172.16.1.23	3351541	03/16/2004 09:55:09

RECONNEX

Status: alpha

Packets: 6302857

Active Flows: 0

Objects Saved: 20383

Storage Avail: 97%

Up-Time: 43.3 days 17:31

Sys. Time: Tue Mar 23 09:13:53 PDT 2004

Tip

Copyright © 2004 ReconNex, Inc.

726

Figure 16

-730

Reconnex Analyze File Edit View Favorites Tools Help
Address: <https://172.16.1.18/analyze/RepreCreateRule.do>
Done

RECONNEX

Status: alpha
Packets: 8392857
Active Flows: 0
Objects Saved: 20383
Storage Avail: 97 %
Up-Time: 433 days 11:26
Sys. Time: Sun Mar 22 09:16:07 EDT 2004

Log Out Analyze Setup Help

Create Capture Rule back to Capture Rules

Capture Rules **Configure System** **Change Password**

Source: IP: Mask Port From Port To
Destination: IP: Mask Port From Port To

Protocol: HTTP Request, HTTP Post, HTTP Webmail, HTTP Webmail Attach

Type: Unknown, JPEG, GIF, BMP

Size: To: 1024, 2048, 4096, 8192
Date/Time From: (pick) Time: mm/dd/yyyy - h:mm
Date/Time To: (pick) Time: mm/dd/yyyy - h:mm

Save Rule: Name: Description: Define Rule

432

730

Figure 17